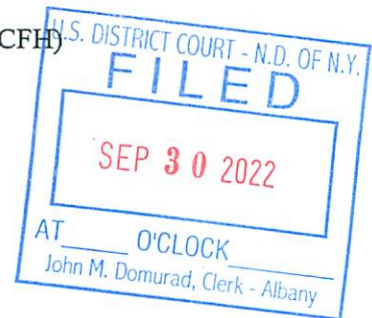


UNITED STATES DISTRICT COURT

for the
Northern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched or identify the person by
name and address)Case No. 1:22-MJ-567 (CFH)

THE FOLLOWING ELECTRONIC DEVICE:

One (1) black iPhone XR bearing IMEI no.
356449109305614CURRENTLY LOCATED AT THE
GREENE COUNTY SHERIFF'S OFFICE AT
45 HAVERLY MEMORIAL DRIVE IN
COXSACKIE, NEW YORK

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 924(c)(1)(A)

21 U.S.C. § 841(a)(1)

Offense Description

Possession of Firearms in Furtherance of a Drug Trafficking
Crime

Possession with Intent to Distribute Controlled Substances

The application is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Joel Rowell #63
Applicant's signature

Joel Rowell, USMS Task Force Officer
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone (specify reliable electronic means).

Date:

September 30, 2022



Judge's signature

City and state:

Albany, New York

Hon. Christian F. Hummel, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION
FOR A SEARCH WARRANT FOR THE
FOLLOWING ELECTRONIC DEVICE:

One (1) black iPhone XR bearing IMEI no.
356449109305614

Case No. 1:22-MJ-____ (CFH)

CURRENTLY LOCATED AT THE
GREENE COUNTY SHERIFF'S OFFICE AT
45 HAVERLY MEMORIAL DRIVE IN
COXSACKIE, NEW YORK

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE

I, Joel Rowell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property — a smartphone — which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer with the United States Marshall Service (USMS), Department of Justice, and have been so employed since October 28, 2021. Accordingly, I am an “investigative or law enforcement officer” within the meaning of Section 2510 (7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code, and Title 21, United States Code.

3. I am also an Investigator with the Greene County Sheriff's Office. I have been a police officer for thirteen years and an investigator for approximately nine years. I have regularly received trainings in conducting criminal investigations and search warrant writing through New York State division of Criminal Justice Services at various locations throughout New York state over the nine years of being an investigator. During my tenure with the Greene County Sheriff's Office, I have had the opportunity to participate in numerous investigations relating to drug trafficking, and have received formal and informal training concerning drug investigations, surveillance, and undercover operations. I have had experience executing search warrants and conducting cellular and computer analysis of devices in connection to a variety of investigations. Through my training, education, and experience, I have become familiar with the manner in which illegal drugs and firearms are imported, distributed, and used in furtherance of criminal activity while attempting to avoid detection by law enforcement.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, analysts and other law enforcement personnel. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. Where statements of others are related in this affidavit, they are related in substance and in part.

5. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 924(c) (Possession of Firearms in Furtherance of a Drug Trafficking Crime) and Title 21, United States Code, Section 841(a)(1) (Possession with Intent to Distribute Controlled Substances) by SAMANTHA STEENBURN and ATNIEL PAGAN. There is also probable cause to search the item described in Attachment A for evidence of these crimes, as described in Attachment B.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched is: one (1) black iPhone XR bearing IMEI no. 356449109305614 (hereinafter, the "DEVICE") possessed by STEENBURN. The DEVICE is currently located at the Greene County Sheriff's Office at 45 Haverly Memorial Drive in Coxsackie, New York.

7. The applied-for warrant would authorize the forensic examination of the DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

Investigation

8. On May 12, 2022, the town of Catskill, New York Town Court issued a warrant for the arrest of ATNIEL PAGAN on the charge of Burglary in the First Degree (New York Penal Law (NYPL) § 140.30). Thereafter, on June 13, 2022, DOCCS issued a warrant for PAGAN for a violation of his parole release conditions. Then, on July 11, 2022, the village of Catskill Justice Court issued arrest warrants for PAGAN on the charges of Assault in the Second Degree (NYPL § 120.05(9)) and Endangering the Welfare of a Child (NYPL § 260.10).

7. On August 17, 2022, at approximately 6:20 a.m., investigators with the USMS RFTF located PAGAN at his residence, 361 Washington Avenue, Apartment 5, in the city of Albany, New York. After observing movement within the apartment through a window, task force members confirmed through neighbors and the property's landlord that PAGAN was the current renter of the residence. After a period of time of knocking and attempting to have the apartment's resident(s) open the door, the door was breached. Task force members then entered the studio apartment, and arrested PAGAN and STEENBURN in the bathroom of the apartment.

9. In the course of arresting PAGAN, task force members observed the following in the common room of the studio: (1) a plastic tie-off baggie containing an unknown amount of what appeared to be cocaine base next to the apartment's only bed; (2) a loaded .223 caliber magazine located on the common room's only table; and (3) a gray and black pistol and magazine on top of a black duffel bag under the table.

10. Albany Police Department (APD) investigators then obtained and executed a search warrant on the premises and recovered, among other things: (1) the gray and black semi-automatic "Polymer80" 9mm semi-automatic pistol equipped with a magazine containing 19 rounds under the table referenced above; (2) a black-and-tan-colored semi-automatic "AREO" AR-style .223 caliber rifle equipped with a fully-loaded 30-round magazine propped against the wall next to the table; (3) four magazines containing a total of 70 rounds of .223 ammunition on the table; and (4) three magazines containing a total of 65 rounds of 9mm ammunition on the table.

11. Also within the studio apartment, investigators recovered: (1) approximately 195 grams of a substance that field tested positive for the presence of cocaine base, packaged in one large baggie, on the above-referenced table; (2) approximately 65 grams of a substance that field tested positive for the presence of cocaine base, packaged in three baggies, on the apartment's kitchen counter; (3) approximately 7 grams of a substance that field tested positive for the presence of fentanyl, packaged in one baggie, on the above-referenced table; (4) approximately 6 grams of a substance that field tested positive for the presence of cocaine base, packaged in five tie-off baggies on the apartment's window sill; and (5) 90 glassine envelopes containing a substance that field tested positive for the presence of fentanyl next to the room's bed. Cocaine Base and Fentanyl are both controlled substances.

12. Inside the apartment's kitchen, investigators recovered paraphernalia of drug distribution, including: (1) four digital scales; (2) four boxes of glassine envelopes, and (3) cutting agent.

13. On the above-referenced common room table, investigators also recovered a cardboard box addressed to STEENBURN containing cutting agent.

14. Electronic devices were observed in the common room, but none were seized.

15. STEENBURN was arrested by APD, charged by complaint with state drug and weapons charges, arraigned on those charges, and was then released on supervisory conditions, including an ankle monitor.

Arrest of STEENBURN on Federal Complaint and Recovery of the DEVICE

16. On September 7, 2022, STEENBURN was arrested on a federal complaint in case number 22-MJ-471 (DJS), when she arrived at the Greene County Correctional Facility to meet with PAGAN, who is presently incarcerated on the pending state charges referenced above. The DEVICE was recovered from her person incident to her arrest.

17. Previously, consensually monitored calls between PAGAN and STEENBURN revealed, in sum and substance, STEENBURN and PAGAN talking about the "food" that STEENBURN is selling and whether or not she is keeping the money or giving it back to "Papi" and other family members of PAGAN. Based on my training, experience and knowledge of this investigation, I know that "food" refers to heroin and/or fentanyl opioid mixtures, and the conversations between STEENBURN and PAGAN appear to depict STEENBURN dealing heroin and/or fentanyl and not retaining the proceeds for herself and PAGAN.

Drug Traffickers and Cellular Devices and Firearms

18. Based upon my training and experience, I know drug traffickers must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their drug trafficking business. For example, many drug traffickers maintain cellular telephones that they use to coordinate their drug trafficking; specifically, they use the cellular telephones to communicate with: (1) suppliers about obtaining additional quantities of drugs and negotiate price and logistics related to acquiring those drugs; (2) customers about available inventory, prices, and logistics related to selling the drugs; and (3) co-conspirators about acquiring, storing, and transporting drugs and proceeds generated from the sale of illegal drugs. Based on my training and experience, I also know that those involved in drug trafficking often use multiple cellular telephones and other electronic devices to facilitate their illegal activities, including access bank accounts, conduct financial transactions, and communicate with co-conspirators about their criminal activities.

19. Based upon my training and experience, I also know drug traffickers to frequently arm themselves with firearms to protect themselves from being robbed of their drugs and/or the proceeds of the sale of controlled substances.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and

from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another

location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP

addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

21. Based on my training, experience, and research, I know that the DEVICE have capabilities that allow them to serve as “a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA.” In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.


24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement’s possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

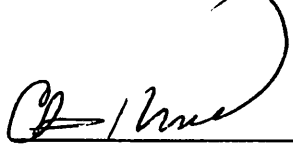
CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the DEVICE described in Attachment A to seek the items described in Attachment B.

Attested to by the affiant,


Joel Rowell
Task Force Officer, USMS

I, the Hon. Christian F. Hummel, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on September 30, 2022 in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.


Hon. Christian F. Hummel
United States Magistrate Judge

ATTACHMENT A

Property to be Searched

The property to be searched is: one (1) black iPhone XR bearing IMEI no. 356449109305614 (hereinafter, the "DEVICE") possessed by STEENBURN. The DEVICE is currently located at the Greene County Sheriff's Office at 45 Haverly Memorial Drive in Coxsackie, New York.

This warrant authorizes the forensic examination of the DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Items to be Seized

All records on the DEVICE described in Attachment A that relate to violations of Title 18, United States Code, Section 924(c) (Possession of Firearms in Furtherance of a Drug Trafficking Crime), and Title 21, United States Code, Section 841(a)(1) (Possession with Intent to Distribute a Controlled Substance) committed by SAMANTHA STEENBURN and ATNIEL PAGAN, including:

Computers and Electronic Media

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and electronic media will be conducted in accordance with the affidavit submitted in support of this warrant.
2. Computer hardware, meaning any and all computer equipment, including any electronic storing devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as thumb drives, flash drives, SD (secure digital) cards, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing, or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).
3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems, software, application software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
5. Computer passwords and data security devices, meaning any devices, programs, or data, whether themselves in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer

hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data, or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents and materials referencing or relating to the above-described offenses. Such records, documents or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as thumb drives, flash drives, SD (secure digital) cards, floppy diskettes, hard disks, CD-ROMs, DVDs, optical disks, printer buffers, soft cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.
7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), or any computer or computer system. The form that such information might take includes, but is not limited to, thumb drives, flash drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, DVDs, video cassettes, and other media capable of storing magnetic or optical coding.
8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding, on computer media, or on media capable of being read by a computer or computer-related equipment, such as thumb drives, flash drives, SD (secure digital) cards, fixed disks, external hard disks, removable hard disk cartridges, CDs, DVDs, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Documents, Records and Evidence

9. Records of personal and business activities relating to the operation and ownership of the DEVICE.

10. Records of address or identifying information for the target of the investigation and any personal or business contacts or associates of his, (however and wherever written, stored or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user ID's, eID's (electronic ID numbers) and passwords.
11. Evidence indicating how and when the DEVICE was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user.
12. Passwords, encryption keys, and other access devices that may be necessary to access any electronic media.
13. Records of or information about Internet Protocol addresses used by seized electronic media, as well as records of or information about the media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
14. Contextual information necessary to understand the evidence described in this attachment.

**Materials Relating to Drug Trafficking and/or the Possession of
Firearms**

15. Any and all chats, chat logs, emails, and other text documents, describing or relating to drug trafficking and/or possession of firearms and ammunition.
16. Any and all address books, names, and lists of names and addresses of co-conspirators engaged in drug trafficking and/or possession of firearms and ammunition.
17. Photographs taken or received by the user of the DEVICE depicting drug trafficking and/or firearms.
18. Records, relating to the source of proceeds deposited to personal and/or corporate bank accounts.
19. Records relating to deposits to personal and/or corporate bank accounts and expenditures of money and wealth, to wit: money orders, wire transfers, cashier checks and receipts, bank statements, passbooks, checkbooks, and check registers.
27. Records related to the purchase of personal assets, including but not limited to real estate, vehicles, jewelry, boats and firearms and ammunition.